# CHAPTER 1

# INTRODUCTION

This chapter provides an introduction to IoT and also explains the significance of the research work. The main intention of this chapter is to determine the security issues of IoT routing. Further, it precisely explains the main contributions of the research work. Moreover, it describes the proposed methodology and thesis outline.

## 1.1 Internet of Things

Due to the proliferation of smart internet-based devices, the Internet of Things (IoT) has gained significant popularity in the modern world. The IoT offers inter-connectivity and smart communication among digital devices such as Personal Computers (PCs), laptops, tablets, smart phones, Personal Digital Assistants (PDAs), and other handheld embedded devices (Atzori et al., 2010) (Jorge et al., 2015). The primary contribution of IoT is to promote connectivity among smart internet devices at anywhere, anytime, anyplace, with anything and anyone ideally using any path/network and any service. Thus, the IoT applications have primarily contributed to day-to-day human activities by enabling smart devices to manage routine life activities and chores. The IoT incorporates a vast amount of heterogeneous devices that are limited in memory, energy, and processing capabilities (Whitmore et al., 2015). Each device in IoT produces diverse data and it is challenging to transmit such huge volume heterogeneous data among the devices. The IoT routing protocols route the heterogeneous data using well pre-defined routing algorithms. However, the internet is the heart of the IoT network and hence, inter-connectivity and security are two major issues of IoT. As a consequence, the quality of data transmissions for future IoT applications is mostly desired in the smart world (Maalel et al., 2013). Hence, the data is interrupted by hackers, malicious activities, and viruses due to the vulnerable characteristics of IoT, such as low computing capability, open network, and high volume data produced by heterogeneous devices.

Currently, the IoT is exploited in a lot of smart social life applications such as smart home security and intelligent transportation system (Ibarra et al., 2017). Although the IoT applications make human life more convenient, it lacks to assure complete security to the personal information of humans that may leak at exuded by attackers at any time. Consequently, attacker stoles or interrupts the signal of IoT once it will straightly damage the security level of the entire IoT system. With the vast exploitation of IoT, it offers a significant level of security according to the application type (Bandyopadhyay and Sen, 2011). The IoT is a proliferated network, and there are no sufficient security solutions to the IoT, resulting in considerable restrictions in the IoT development. Therefore, it is essential to propose meaningful security solutions to IoT routing protocols. A prominent routing mechanism, named as the Routing Protocol for Low Power and Lossy Networks (RPL) is a standardized routing mechanism proposed for IoT. However, the RPL is a fundamental routing solution primarily proposed for IPv6 over Low Power Wireless Personal Area Networks (6LoWPAN) is vulnerable to several types of security attacks (Wallgren et al., 2013). It suffers from offering high-quality security to the IoT and it is crucial to develop security solutions against various types of attacks against RPL.

## 1.2 Significance of IoT

The management department of a city officially interacts on handling smart city infrastructure, and the department of government has to solve the real-time issues facing by each city citizen in every day of life (Zanella et al., 2014) (Talari et al., 2017). The city management department has to monitor the activities happening in the city for providing admirable life quality to its citizens. IoT is a new rebellion of the Internet in which the intelligent devices that make self-assisted internet-enabled communications among them and also improves the human lifestyle precisely. Due to the elevation of improving life activities better, the IoT is considered as a significant frontier for human life. The IoT also networked the devices that are not formerly connected and responses to such devices as smart devices. The growth of IoT has to revolutionize the entire world in 2020 (Gartner, 2013). Nowadays, IoT technology plays a significant role in human life, and it reinvents daily funs. Thus, the IoT creates a revolutionary transformation in both the digital and IT world, and also it enhances the potential for touching everyone's life day by day. The devices of IoT can rectify the issues related to traffic, crimes, noise, and pollution. It also

maintains the assets that are IT security, intelligent transportation system, schools, industries, hospitals, power plants, water supply management, garbage management, law enforcement, and other industrialized society services to local government departments.

### 1.3 IoT Security Challenges and Requirements

Generally, IoT comprises a vast amount of connected devices, and such devices produce a large amount of heterogeneous data in the network. Thus, it increases the IoT complexity and also boosts the security challenges of IoT. Due to the limited battery power and low memory capabilities, most of the IoT devices lack to include malware protections and it increases the vulnerabilities in the network (Noor et al., 2018). Consequently, the IoT devices are easily affected by the attackers due to their heterogeneity and unprotected software. Once an attacker compromises the IoT device, it takes over the control of the entire IoT system and creates a significant influence on the routing functionalities of the IoT system. In addition, the resource-constrained nature of IoT devices immensely aggravates the system performance in the presence of malicious activities. Detecting such malicious activity promptly assists in maximizing the routing efficiency and also enhances the overall network performance. Some of the security challenges in IoT routing are as follows.

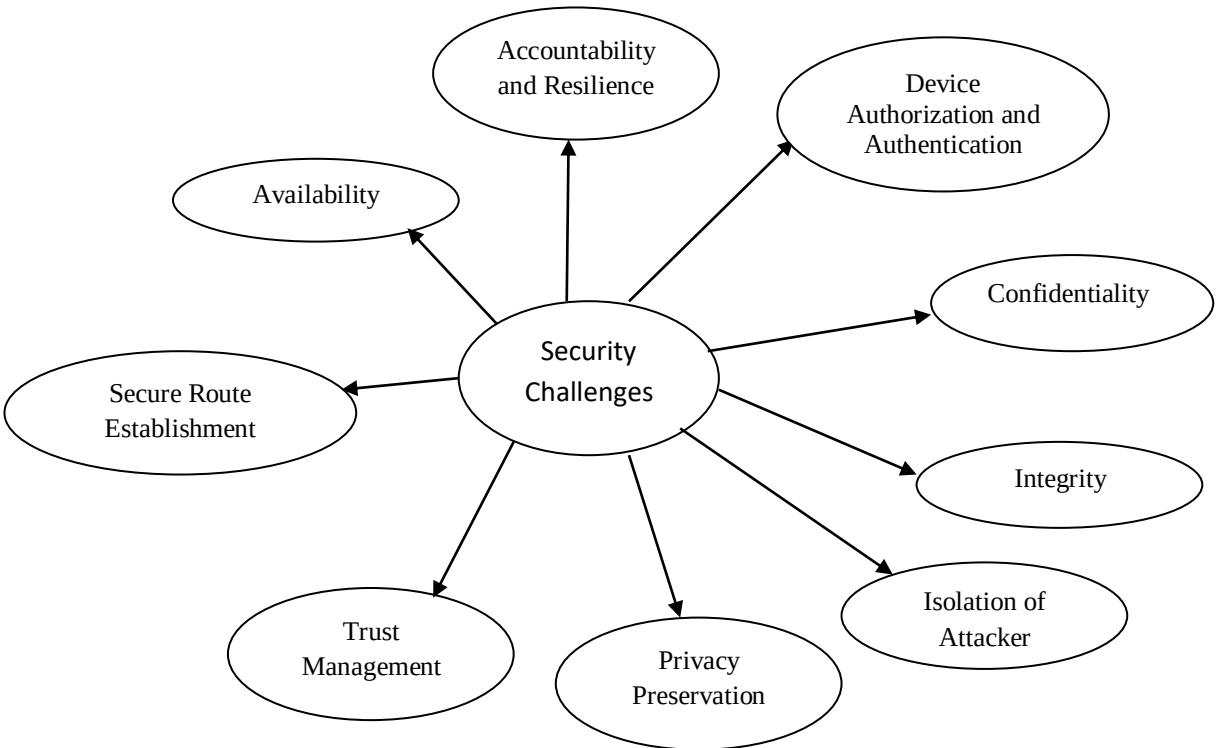

**Figure1.1: Security Challenges of IoT**

**Device Authorization and Authentication:** It is essential to ensure security for the IoT system. The IoT devices have to establish authorized identities to access gateways and establish communication with other IoT devices. The devices also have passwords on a weekly basis or preamble manner for application services.

**Confidentiality:** It is significant to assure that the IoT information is secure, and the data is only available for authorized devices. It is a heterogeneous network since the devices are actuators, machines, services, and humans. For example, the sensors do not reveal the retrieved and collected information to the other nodes in wireless sensor networks. Another confidentiality issue is data management in which the data is securely routed to the destination using some secure routing protocols.

**Secure Route Establishment power-constrained Devices:** It is a main challenging issue in IoT routing protocol design. The IoT routing protocol should able to determine a secure routing path for data transmission among two communicating devices. The computations exploited for secure routing path discovery must be lightweight, as the IoT devices are naturally power-constrained, and such low power devices have to solve the security issues.

**Integrity:** In IoT, the data is exchanged between various heterogeneous devices in which the quality of data is an important issue. The integrity assures that authorized devices forward the data and also ensures that data should not be tampered during transmission. Moreover, integrity maintains end-to-end security among the communication devices of IoT. The devices are low battery-powered in IoT, and hence, it is essential to assure integrity using lightweight solutions.

**Isolation of Attack behavior:** It is a significant challenge in IoT routing to detect the attack and isolate the attacker nodes. It is crucial to detect malicious activities rapidly and robustly for enhancing IoT performance. The IoT routing protocol can detect malicious activity in the network. Current IoT routing mechanisms are mostly insecure, as they are not taking into

account the IoT inherent characteristics in protocol design. Moreover, there is a need to design efficient routing techniques with high-security solutions for the IoT environment.

**Privacy Preservation:** The personal information such as location and the real identity of devices are very sensitive, and it is crucial to preserve that private information during IoT routing and attack detection. Secure routing protocols must have the ability to detect malicious activities without revealing the personal information of the IoT devices.

**Availability:** Availability ensures that the data or devices are available whenever they are requested by the authorized users and services. The IoT devices have to work robustly providing services even in cases of any malicious intrusions or adverse situations. The severe security threats that affect the availability of data or services are DOS attack, packet dropping attack, resource depleting attack and other routing attacks. Each application has its unique availability requirements. For instance, applications such as healthcare monitoring and fire monitoring, the continuous availability of data and users are essential as otherwise, it leads to life-threatening situations.

**Trust Management:** Trust management aims to ensure secure access control by detecting and eliminating malicious nodes in the network. Due to the vulnerability in IoT devices, dynamic trust management protocols are suitable for accurately differentiating cooperative and non-cooperative nodes. The trust management in IoT has to consider device trust, data trust and entity trust. Among them, the device trust is a challenge, as the ability to confirm the prior originality or trust ability of the devices is difficult. Therefore trusted computing approaches are applied for standardized devices for establishing the device trust. Apart from this, due to the possibility of both homogenous and heterogeneous devices in the network, a different trust mechanism has to be adopted based on the devices. Entity trust refers to the trustworthiness of participants such as persons or services. Unlike trusted computing in device trust, behavioral attestation based approaches are needed in determining the entity trust, which is more challenging and experimental. Considering data trust in IoT, the application of data aggregation and machine learning techniques helps in retrieving the trust data from the potentially untrusted devices.

**Accountability and Resilience**:**:** Accountability symbolizes that the particular operations performed are clearly bound to authenticated entities. Accountability is helpful in ensuring that the security techniques are working correctly, in spite of the advantages IoT faces problems to provide better accountability due to the considerable amount of devices, access delegation and

multiple organizational domains. In case of a repudiation incident, the accountability process is useful in checking the in-depth information on the actual occurrence of the incident. The scalability of IoT leads to the possibility of attacks and failures due to the various hardware and software employed. Hence it is necessary for the system to support and recover in case of any crash during data transmission

### 1.4 Security Threats against RPL in IoT

The heterogeneous IoT devices are restricted in battery power, memory, and computation capabilities. Due to the ubiquitous nature of IoT, it is vulnerable to several types of attacks, as discussed in (Wallgren et al., 2013) (Jiang et al., 2018). Therefore, security plays a vital role in IoT. There are several security attacks in the RPL network, and each attack establishes its malicious activities based on the network topology, network traffic and resources (Mayzaud et al., 2016). Based on the topology, there are several types of security threats such as selective forwarding, sinkhole, hello flooding, wormhole, black hole attack, and Denial of Service (DOS) attack. Based on network traffic, the security threats are sniffing, traffic analysis, decreased rank attack, and Clone ID and Sybil attack. Based on the resources, the security threats are flooding, routing table overhead, increased rank attack and DAG inconsistency.

**a) Classification based on Topology:**

**Selective Forwarding:** In this type, the attacker also selectively forwarding the packets to the destination, and drop the remaining packets during the transit. For instance, the attacker forwards the control messages of RPL correctly, whereas it mainly drops the data packets.

**Sinkhole Attacks:** In this type, an attacker builds artificial routing paths and launching the attack by transmitting the data traffic through the established artificial routing paths. The sinkhole attack does not create a more significant impact on RPL routing operations,

as long as the attacker is separated. However, when the attacker is coupled with various types of attacks, it creates a severe impact on routing operations.

**Hello Flooding:** Every node in IoT routing exploits hello packets for route establishment and data forwarding. In hello flooding attack, an attacker broadcasts unnecessary hello packets within the network in order to launch an attack by pretending as a neighboring device as many devices. The data packets are highly loosed in the presence of hello flooding attackers, as the source believes the flooding attacker is its neighbor for data forwarding, whereas the attacker is in out of communication range of source.

**Wormhole Attacks:** The wormhole attacker creates an out of band connection among two devices by exploiting wired or wireless communication links. The wormhole attack paths are rapidly forwards the data packets compared to typical routing paths. The wormhole attacker does not create strong influence until it is combined with other types of attackers in the network.

**b) Classification based on Network traffic:**

**Clone ID and Sybil Attacks:** In the Clone ID attack, an attacker obtains the real identities of other devices, and it launches an attack by pretending as multiple devices in the network. In other words, an attacker node clones the identity of another existing node to gain access to traffic destined to that victim node. To create this attack, malicious nodes are selected and all of the node's properties such as rank IDs and numbers are added to it. Likewise, the Sybil attacker reinforces a malicious event within the network and it motivates the devices to take wrong routing decisions. This type of attack creates a great influence on trust-based security solutions. The Sybil attacker can control a large part of the network by pretending as multiple devices and it reduces the overall system performance.

**Sniffing Attack:** Sniffing attack launches the attack passively without disturbing the services of the network. These attacks aim to steal sensitive information, thereby compromising the confidentiality of the communication. The sniffing attack is performed through a compromised device or captured directly through the shared medium in the network.

**Traffic Analysis:** Traffic analysis attack mainly targets in obtaining the routing information by considering the characteristics and traffic patterns of the network . If the presence of a traffic analysis attacker is near the root node, the attacker is able to obtain the routing information of almost all the edge nodes and launch other serious attacks in the network.

**Decreased Rank Attack:** In the RPL protocol, rank property depicts the location of each node within the DODAG. Rank plays a significant role in avoiding and detecting loop formation in the network. In specific, the rank of the nodes increases from the sink to leaf nodes in a downwards direction and the low ranking node is selected as the parent node. In rank attack, malicious nodes change the rank rule by posing themselves as the lowest rank for entering the parent selection. The neighboring node that receives the rank of the malicious node in the DIO packet elects the attacker as its respective parent node. These attacks are launched primarily before routing attacks such as sinkhole attacks for becoming part of the routing path.

**c) Classification based on Resources:**

**Denial of Service Attacks:** The DoS attack is one of the serious threats that disrupt the services in the network by continuously flooding fake data packets. In DDoS attacks, multiple attackers incur spurious data transmissions towards the targeted node or gateway node. These flooding attackers continuously send fake data packets to the gateway node for disabling it from performing its services. In case, a normal node sends packets to the gateway node, these packets are dropped, and the gateway node keeps on receiving the flooding packets.

**DAG Inconsistency Attack:** In a DAG inconsistency attack, the attacker node uses the datapath validation mechanism in RPL for launching the attack. The malicious node manipulates the RPL IPv6 header options to present a fake existence of DAG inconsistencies forcing the target to drop packets. This attack causes an RPL router to reset its DIO Trickle timer and thereby frequently transmitting DIO messages. It leads to a DoS attack, which increases the control overhead and energy consumption in the network.

**Version Number Attack:** In version number attack, the attacker node presents itself with the higher version number of the DODAG tree. When nodes receive the new higher version number in the DIO message, the DODAG tree formation is reconstructed. This causes the generation of new unoptimized topology and brings inconsistencies in topology.

## 1.5 Scope of the Research

IoT receives excellent attention, and it becomes a cardinal of the research community (Ning and Wang, 2011). Nearly 26 billion devices are going to connect to the IoT network worldwide by 2020 (Gartner, 2013). The primary devices of IoT are diverse kinds of things that are humans, actuators, ITS, sensors, and mobile phones. The advantage of IoT in the modern IT world has witnessed in various kinds of applications of human's everyday life (Zanella et al., 2014) (Hancke et al., 2012) (Kyriazis et al., 2013). Due to the diversity and dynamic nature of IoT applications, security is a prominent requirement. The popularity of IoT has increased significantly due to minimum cost, speed of internet availability, large range acquisition of Internet Protocol (IP) based devices, minimum cost sensors, and novel data analytics algorithms. RPL is a popular IoT routing layer protocol, and it builds routes to forward the information to IoT gateway successfully. The IoT major requirements of IoT are end-to-end device connectivity, the establishment of routing paths, filter and process the information, security, and protocol management. The IoT devices are resource-constrained in terms of better memory and processor, and thus, it poses several security issues in IoT routing. Hence, the problems associated with secure routing should be solved to improve the safety and seamless IoT functionality. Although the IoT offers a vast amount of benefits, the insecurity of the protocol design is a prominent issue. The IoT is a rapidly proliferated technique and traditional routing mechanisms are not suitable to address the security issues of IoT.

## 1.6 Problem Statement

In IoT, the presence of dropping attackers significantly disrupts the routing protocol functionality and increases the packet loss rate in the network. Secure routing is complex while handling two

specific routing issues. Firstly, the applicability of heavy-weight security solutions in IoT is disputable, due to severe restrictions on node resources. Secondly, the trust measurement itself comes from unproductive due to context-independent routing behavior observation. In IoT, harsh channel conditions such as network collision, lossy link cause packet drops in the network. Hence, examining the packet loss rate is not adequate to precisely identify the packet loss due to malicious activities. To handle this problem, some of the existing works have extended the RPL routing protocol, which adopts the routing behavior observation to cope with malicious activities. However, the malicious nodes candidly observe the knowledge from routing activities, and it can camouflage its malicious behavior under the background of collision dropping. Also, as the rank is the critical factor in deciding the parent node in RPL, the malicious node purposely announces a small rank value, and as per the RPL, several nodes may get selected as a parent node. Under such a situation, a malicious node appears to be benign, even when it drops the numbers of data packets; the packet dropping due to malicious behavior is misclassified as collision dropping. It implies that the general context-aware trust model is not directly applicable to RPL routing. Therefore, it is more important to precisely decide whether the misbehavior is distinctively due to malicious activity or network constraints.

## 1.7 Research Contributions

In order to ensure high security against various types of RPL attacks, this work proposes five different methodologies that offer diverse security solutions against various types of attacks. The main contributions of the proposed methodologies are as follows.

### 1.7.1 Contributions of TDD and SLTD

- The main intention of Trust-based DDoS Detection (TDD) and Subjective Logic-based Trust Mechanism against DDoS (SLTD) are to design a trust-based secure routing protocol for IoT against DDoS attacks. By incorporating appropriate trust detection mechanisms, the TDD

and SLTD detect the attackers efficiently. Thus, it significantly improves the RPL performance. Figure 1.2 represents the block diagram of Trust-based detection mechanisms against the DDoS attack.

- In order to evaluate the trust value accurately, the TDD mechanism adopts a data frequency-based behavior observation. The utilization of gateway nodes in final trust evaluation enhances the detection accuracy and minimizes the power consumption in TDD.
- The subjective model in STLD adequately reflects the uncertainty in evidence collection and improves the trust accuracy level. By integrating both direct and indirect trust values in trust evaluation, the STLD mechanism improves the attack detection rate and routing efficiency.
- Finally, the performance of both TDD and STLD routing protocols is evaluated using a Cooja simulator. The effectiveness of the proposed techniques is analyzed using diverse performance metrics and diverse scenarios.

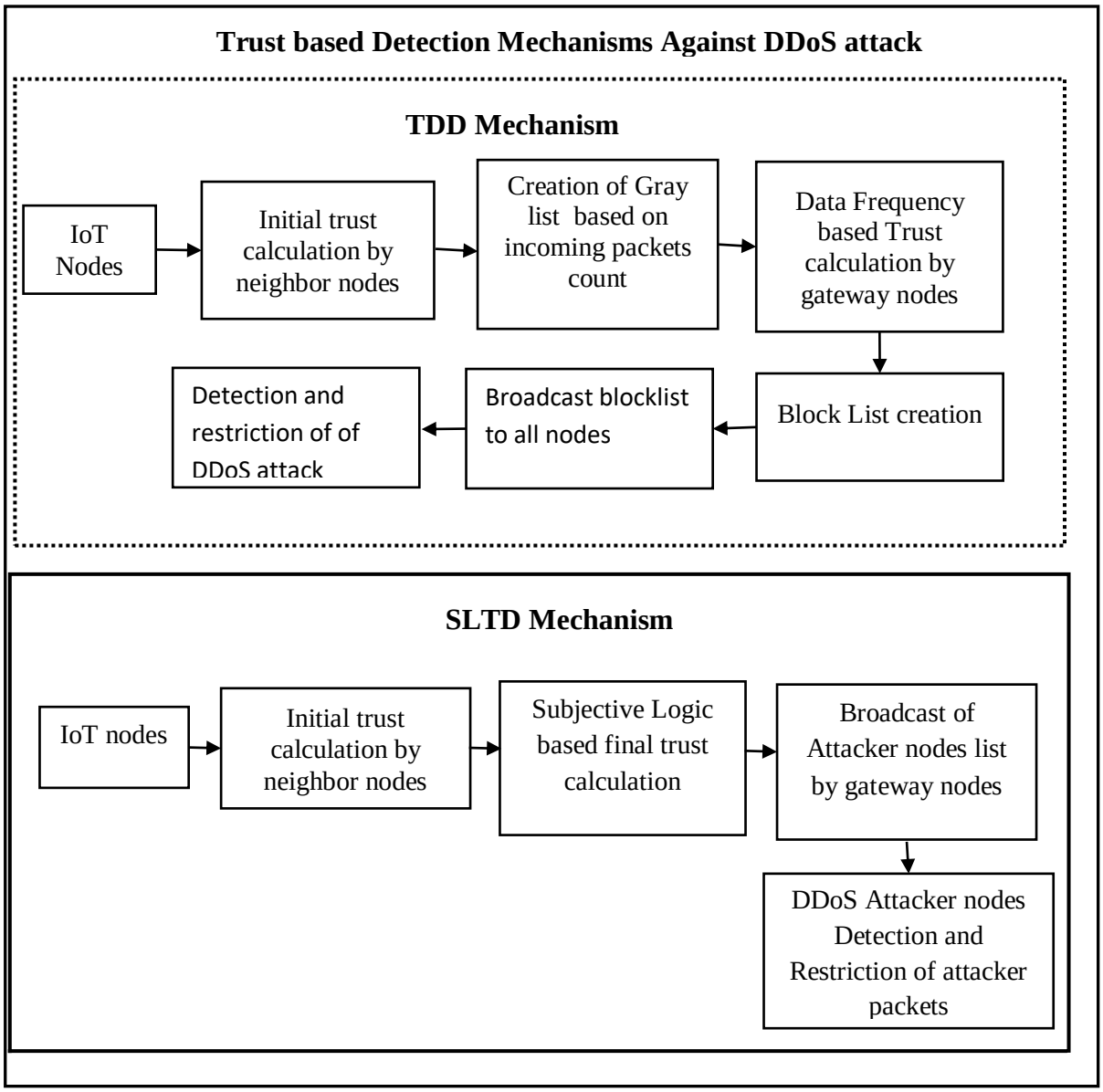


**Figure 1.2: Block Diagram of Trust-based detection Mechanisms against DDoS Attack**

### 1.7.2 Contributions of TSF-RPL and MLT-IoT

- To detect selective forwarding attacks and improves the RPL efficiency, the Trust-Based Selective Forwarding Attack Detection in RPL (TSF-RPL) and Multi-Level Trust-Based Secure RPL over IoT (MLT-IoT) mechanisms are designed. Figure 1.3 presents trust based detection mechanisms against selective Forwarding attacks.

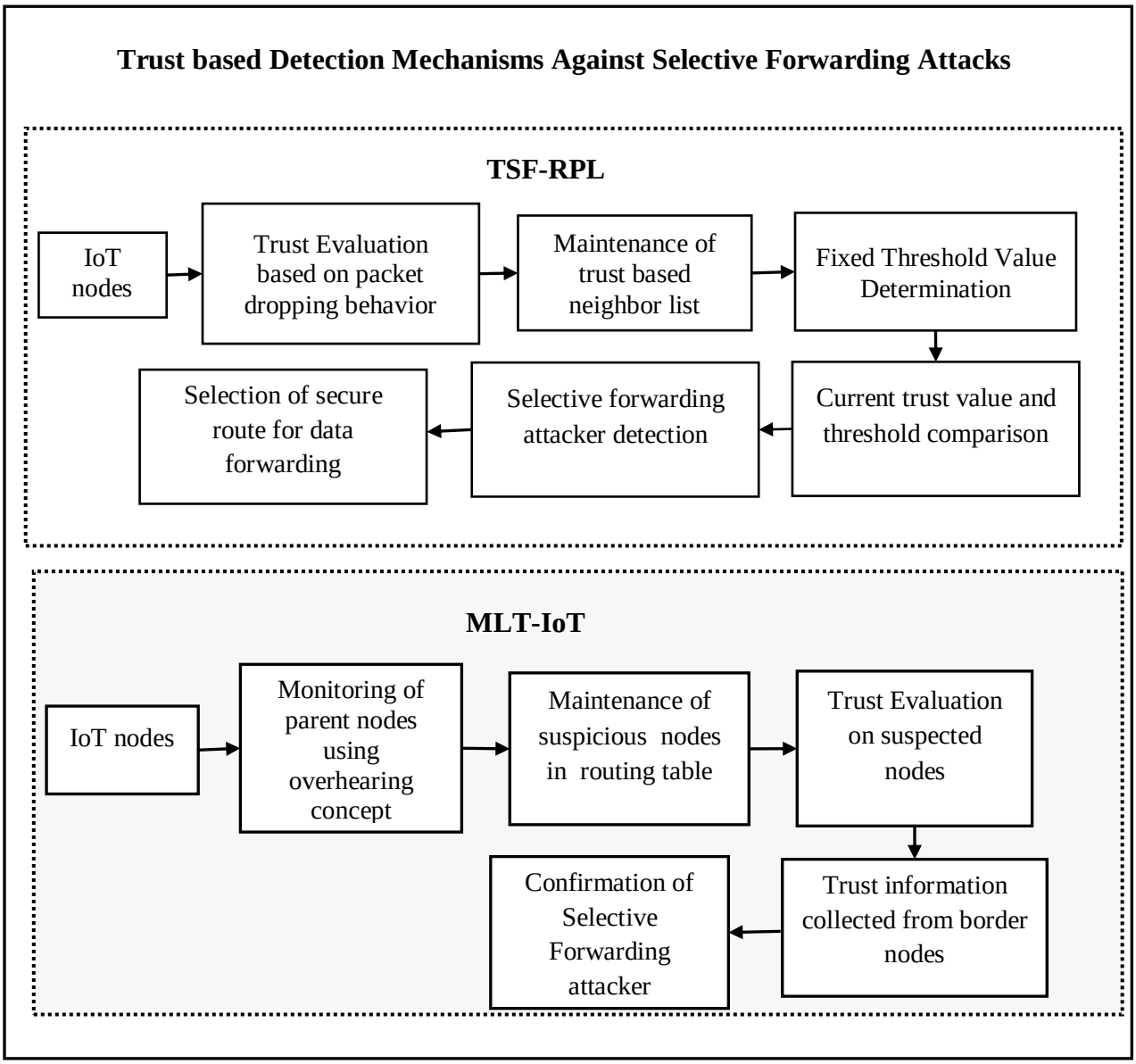


**Figure 1.3: Block Diagram of Trust-based Detection Mechanism Against Selective Forwarding Attack**

- By observing the node behavior continuously, the TSF-RPL mechanism estimates the packet drop rate of neighboring nodes, and it exploits gateway in attack behavior confirmation. Thus, it increases the detection rate with minimum power dissipation.
- Evaluating the node trust in multiple levels, the MLT-IoT neglects the trust inaccuracy due to

abnormal network conditions. The gateway nodes in MLT-IoT collect a second level opinion from border nodes in attack confirmation that improves the attack detection rate.

- Moreover, the Cooja simulator is employed to estimate the performance of both TSF-RPL and MLT-IoT. The performance is observed in terms of detection accuracy, power consumption, overhead, and throughput.

### 1.7.3 Contribution of S-MODEST

- The proposed work aims to adapt the Secure RPL using non-cooperative game MOdels and DEmpster Shaffer Theory (S-MODEST) to IoT routing specifications, detect the malicious attacks, as well as to self-enforce the routing cooperation of nodes using a lightweight security scheme. (Figure 1.4)
- The Non-cooperative game theory formulates the interactions between players using non-zero sum game theory, and it assists the evolutionary game theory in measuring the DODAG and RPL-specific contextual trust value.
- The consideration of interactions and RPL-specific rank variance in contextual trust measurement avoids the camouflage of malicious nodes under the background of collision dropping and improves the trust accuracy in the IoT environment.
- The restricted Dempster-Shaffer theory collects and validates the selective evidence of neighboring nodes without increasing the false positive rate and routing overhead.
- The self-enforcement concept in the non-zero sum game theory enables S-MODEST for the fast convergence of IoT devices to Nash equilibrium and improves the network performance.
- The consideration of accumulated trust of the entire path in the evolutionary game model enables S-MODEST to extend the trust advantage and attain better throughput in RPL routing. The performance of the S-MODEST is evaluated using the Cooja simulator.

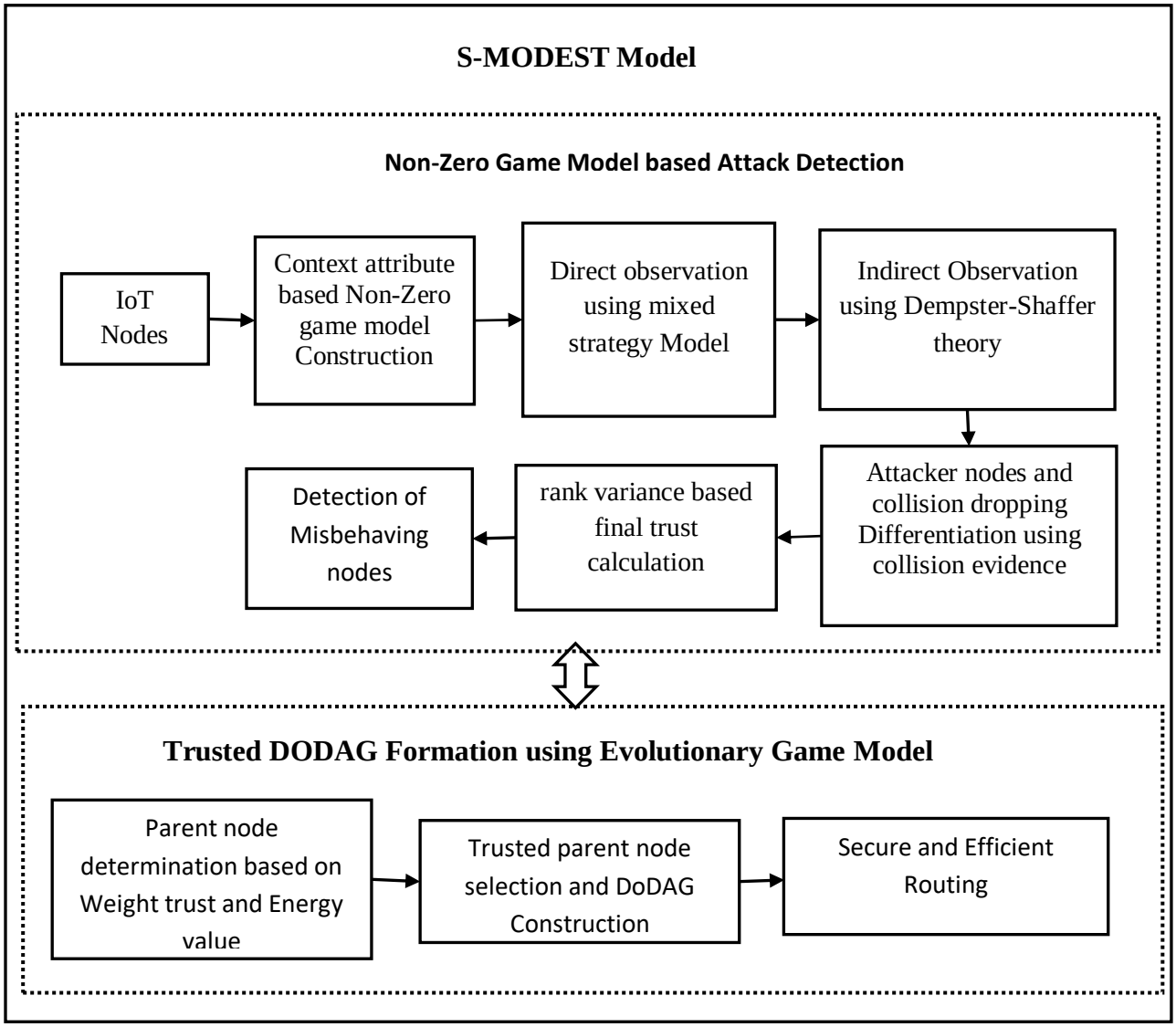


**Figure 1.4: Block Diagram of S-MODEST Model**

### 1.8 Thesis Outline

The remaining chapters of the thesis are organized as follows.

**Chapter 2** briefly describes the background and a literature survey of RPL routing. In the background, the fundamental architecture of IoT with different IoT technologies and applications

are explained in detail. It also explores the various IoT routing protocols and security challenges. Further, it provides conventional secure routing solutions. Finally, it surveys the papers related to the proposed secure routing solutions and compares the existing works with their advantages and limitation.

**Chapter 3** proposes two different trust based RPL security mechanisms named as TDD and SLTD against DoS attack. Firstly, it explains the protocol design and trust evaluation of the TDD mechanism with data frequency-based attack detection methodology. Consequently, it demonstrates the performance setup with the evaluation results of TDD with appropriate graphs and descriptions. Secondly, it explores the process of the subjective logic-based trust evaluation method of SLTD against the DoS attack. Moreover, it shows the simulation parameters with different routing metrics and evaluates STLD by comparing it with appropriate existing techniques.

**Chapter 4** offers significant trust-based security mechanisms that are TSF-RPL and MLT-IoT against selective forwarding attacks. Initially, the designing methodology of TSF-RPL and attack detection mechanisms is explained in detail. Further, the performance evaluation of TSF-RPL is depicted with appropriate results and descriptions. Secondly, the MLT-IoT mechanism is explained comprehensively with adequate formulations. Moreover, the performance of MLT-IoT is estimated and its effectiveness is analyzed by varying different network scenarios and comparing it with the suitable existing solution.

An adaptive lightweight security model named as S-MODEST has been proposed in **chapter 5.** The lightweight model exploits non-cooperative game theory and context-aware trust model for selecting the routing misbehaviors. Consequently, the effectiveness of S-MODEST has been evaluated using the Cooja simulator. The simulation demonstrates the simulation setup, performance metrics, simulation results, and detailed descriptions. Finally, the utilization of restricted Dempster-Shaffer theory in S-MODEST efficiently balances the accuracy of trust evaluation and overhead.

**Chapter 6** concludes this thesis and also describes the possible future directions of secure RPL routing over IoT.